U.S. Department of Energy
Office of Electricty Delivery and Energy Reliability

October 2008

Protecting Process Control Systems Against Lifecycle Attacks Using Trust Anchors

Trust anchors are functional elements that can be introduced into control systems to provide unbiased measurement and unimpeded control capabilities

Introduction

Critical infrastructure control systems are vulnerable to physical and cyber attack. Securing these systems is a top priority for the United States, but none of our efforts adequately addresses a fundamental and extremely dangerous vulnerability: The entire lifecycle of these commercial-off-the-shelf (COTS) systems, from design and production to maintenance and security management, is primarily under the control of foreign nations. Our adversaries have ample opportunity to compromise our critical systems at every stage of those systems' lifecycles.

We suggest a fundamentally different approach for ensuring process control system security. We introduce the concept of a *trust anchor*—an independent monitoring and control device that has access to a component's inner workings—that may be integrated into an untrustworthy system to inspect and verify its function at the lowest level.

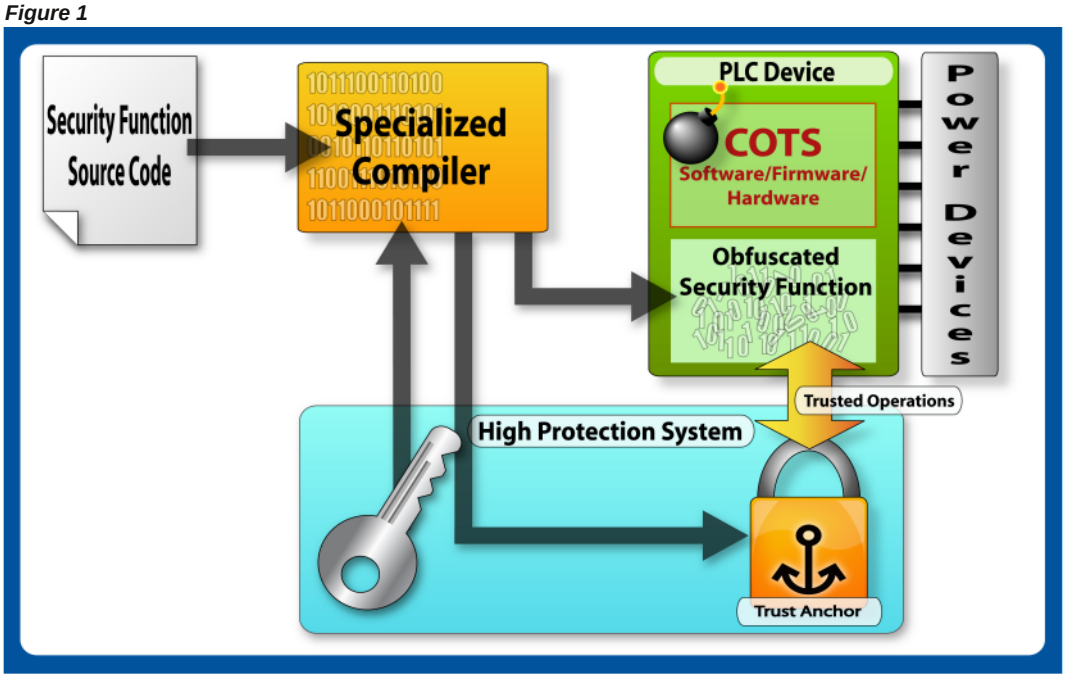
Trust Anchors

We propose the use of trust anchors to address the threat posed by foreign control of the process control system lifecycle. Trust anchors provide verification that systems function correctly, can assume control to ensure correct operation, and provide a foundation for additional, independent security services.

Capabilities

Trust anchors provide two core services—unbiased monitoring and unimpeded control—that provide a flexible foundation for multiple security services. The ability to provide unbiased measurements at the lowest levels of a system enables trust anchors to independently verify system function, reveal deceptive malicious function, independently attest to system state, and verify the correctness of system tests. Trust anchors' control capabilities make it possible to implement trusted control functions, remove discovered malicious content, execute system tests, and conduct experiments on and analysis of a suspected compromise. A trust anchor at the lowest level of a system provides a root of trust, and additional trust anchors can be promoted dynamically to ensure correct operation at all levels of abstraction.

Figure 1



Trust Anchors

Threat Model

- Our adversaries control commercial hardware and software supply chains
- Our adversaries have ongoing access to our systems through administration, configuration, and updates
- Our adversaries rely on our inability to deeply inspect our systems and make unbiased measurements
- Our adversaries rely on complexity and our resulting inability to analyze our systems
- Our adversaries rely on these collective information technology (IT) weaknesses as an avenue to attack U.S. strengths

Security Properties

- Adversaries cannot be aware of what the device is measuring
- Adversaries cannot understand the function or modify it
- Adversaries cannot subvert the system, as any modification will be immediately evident

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Secure Obfuscation Technology

Sandia's secure obfuscation technology (Figure 1) is mathematically provable obfuscation that enables some of our trust anchors' most important capabilities. Code obfuscation is an active area of academic research, but most findings have merely demonstrated that general obfuscation is impossible. By modifying the security model such that we may rely on the presence of a small, tamper-protected device, however, Sandia has developed an effective method for obfuscating code.

Secure obfuscation technology enables one of the most important capabilities of trust anchors: It obfuscates trust anchors' functions and renders them tamper-proof in a cryptographically secure manner. This obfuscation enables the trust anchor to test a system for correct behavior in such a way that an adversary will not have predictable test vectors to work around, which greatly increases the risk to an adversary intending to insert malicious function.

Trustworthy Process Control Systems

Introducing trust anchors into otherwise untrustworthy process control systems affords both a higher level of confidence in the correctness of a system and the ability to assume control of a system to ensure correct operation. Once this concept has been demonstrated and proven, we envision ubiquitous use of trust anchors in process control systems to ensure security.

While trust anchors' protective functions will make the process control system lifecycle harder to compromise, the unpredictable nature of the tests the trust anchors will execute, made possible by Sandia's secure obfuscation technology, will greatly increase the risk to an adversary attempting to effect such a compromise. Under current security models, an adversary can assess the risk of an operation and make an informed decision about whether to proceed with an attack based on an estimable cost, benefit, and risk. Trust anchors affect such risk analyses in two ways: First, trust anchors serve as an effective defensive technology, and will increase the probability of an attack failing or being detected. Second, because trust anchors are obfuscated and an adversary therefore cannot predict their behaviors, they add uncertainty to any adversary's risk analysis equation. If the probability of success or failure cannot be accurately quantified, risk assessment and decision-making processes are made much more difficult.

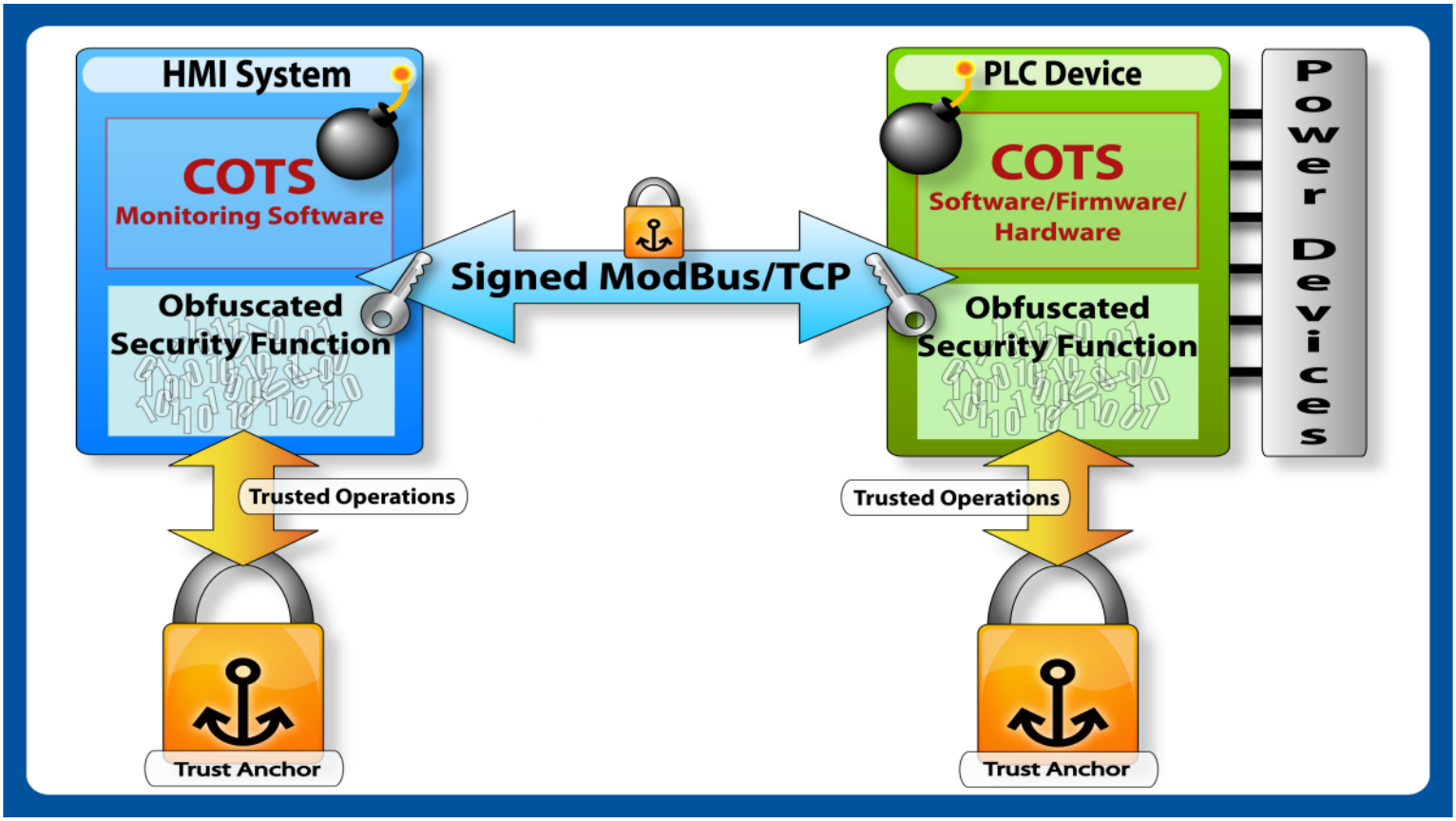
Trust Anchors Preventing Attack

Even when all COTS components in a system prove untrustworthy, trust anchors can be used to ensure the components behave correctly and to establish secure communication among them. Figure 2 demonstrates how trust anchors can be used to ensure proper behavior and secure communication between two untrustworthy COTS components.

Trust Anchors as a Fail-Safe

In the event that a trust anchor uncovers a reason that a process control system component cannot be trusted, the trust anchor can immediately assume control of process control systems and provide fail-safe, reduced-functionality control capability. For example, if a component misreports a sensor reading (intentionally or not), a trust anchor would have the capability to report the correct reading, raise an alarm, and, if necessary, take over all component functions.

Figure 2



Example of trust anchor technology implemented on a COTS HMI and PLC to create a trusted ModBus communication

For More Information: Robert Hutchinson 505.844.4131 rlhutch@sandia.gov